



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/706,871	11/12/2003	Nicholas Stamos	3602.1000-002	6738
21605	7590	01/12/2009		
HAMILTON, BROOK, SMITH & REYNOLDS, P.C.				EXAMINER
530 VIRGINIA ROAD				MURDOUGH, JOSHUA A
P.O. BOX 9133			ART UNIT	PAPER NUMBER
CONCORD, MA 01742-9133			3621	
			MAIL DATE	DELIVERY MODE
			01/12/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)
	10/706,871	STAMOS ET AL.
	Examiner	Art Unit
	JOSHUA MURDOUGH	3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If no period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 9/11/2008.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-22 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-22 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO/SB/08)
 Paper No(s)/Mail Date 9/25/2008

4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____
 5) Notice of Informal Patent Application
 6) Other: _____

DETAILED ACTION

Acknowledgements

1. This action is responsive to Applicants' amendment received 11 September 2008.
2. Claims 1 and 12-22 have been amended.
3. Claims 1-22 are pending and have been examined.

Information Disclosure Statement

4. There are 3 pages in the Information Disclosure Statement ("IDS") received 25 September 2008. They are numbered "1 of 1," "1 of 2," and "2 of 2." The page numbered "1 of 1" has the incorrect inventor and filing date on it. Moreover, the references on it are to medical devices. The Examiner believes this sheet and the corresponding references were included by mistake. However, the Examiner has considered the references in the IDS.

Specification

5. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 C.F.R. §1.75(d)(1) and MPEP §608.01(o). Correction of the following is required:

- a. "kernel events" as recited in at least claims 1 and 12.

Claim Rejections - 35 USC § 112 1st Paragraph

6. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it

pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claims 1-22 are rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

8. Claims 1 and 12 have been amended to include the limitation, “atomic events being low level kernel events.” Applicants have provided a list of atomic events in Figures 4A-B. Nowhere in the specification nor the figures is it recited that atomic events are kernel events. Moreover, as can be seen in Figure 4B, some of the events are described as being high level. Therefore, even if it was decided upon review that the atomic events are kernel events, Applicants' have clearly shown that they are not all low level events, as is stated in the claims.

Claim Rejections - 35 USC § 112 2nd Paragraph

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 1-22 are rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

11. As noted above, Applicants have shown “atomic events” to be both low and high level events in Figures 4A-B. In claims 1 and 12, as currently amended, atomic events are stated to be low level kernel events. One of ordinary skill in the art would not understand if the events

shown as "Action Type" 26-43 in these figures are low level atomic events as stated in Applicants' specification (Page 6, line 5) or high level as indicated in the figures.

12. Similarly, the events shown as "Action Type" 1-25 are shown as being low level events in the figures, but are also described as being "typical high level event patterns" in Applicants' specification (Page 11, line 10).

13. The Examiner has reviewed Applicants' specification and has been unable to find a definition with sufficient deliberateness, clarity, and precision to lexicographically define "atomic events."

14. Given the lack of definition and conflicting explanations in the specification the attempt to define the phrase "atomic events" as being "low level kernel events" in the claims would render one of ordinary skill in the art unable to ascertain what is needed to infringe on this limitation.

15. Claims 1 and 12 also recite, "sense/sensing atomic events from within an operating system kernel of a user client device." One of ordinary skill in the art would find this unclear as to whether the sensing is occurring in the kernel or if the events are from the kernel. The Examiner has interpreted the latter to be the case.

Claim Rejections - 35 USC § 102

16. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless —

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an

international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

17. Claims 1-5, 7, 8, 10-13, 15, 16, 18, 19, 21, and 22, as understood by the Examiner, are rejected under 35 U.S.C. §102(e) as being anticipated by Carter et al. (US 2003/0051026) (“Carter”).

18. As to claim 1, Carter shows:

An agent process for controlling access to digital assets in a network of data processing devices, the process comprising:

defining a security perimeter **114** that includes two or more data processing devices (protected servers, figure 1);

defining one or more policy violation predicates (Paragraphs 0775-0783) that serve to implement policy logic and that are asserted upon an occurrence of a possible risk of use of a digital asset by an end user outside of the security perimeter (Paragraphs 0787-0791 and tables included within);

sensing atomic events (listed after paragraph 0787) from within an operating system kernel of a user client device (“workstation,” Figure 1) (Paragraph 0810), the atomic events being low level kernel events and being sensed upon activities related to authorized access (Paragraph 0811) (through switch controlled by the Network Surveillance and Security System, “NSSS” **18**) to a digital asset (located on a protected server within group **114**) by the end user of the user client device; aggregating multiple atomic level events to determine a combined event (Paragraph 0435); and

asserting a policy violation predicate upon an occurrence of a combined event that violates a predefined digital asset usage policy that indicates a risk of use of the digital asset outside (inherent because the workstation is outside of the secure switch) of the security perimeter (Paragraph 0435).

19. As to claim 12, Carter shows:

A system for controlling access to digital assets in a network of data processing devices, the system comprising:

a digital asset usage policy server **18** storing one or more digital asset usage policies (Paragraphs 0787-0791 and tables included within) configured to be applied to a security perimeter **114**, the security perimeter comprising two or more data processing devices (protected servers, figure 1);

an atomic event sensor (things sensed are listed after paragraph 0787, therefore there is inherently a sensor), the sensor located within an operating system kernel (Paragraph 0810) within an end user client device (“workstation,” Figure 1) and configured to sense atomic events from within the operating system kernel (Paragraph 0810), the atomic events being low level kernel events and being sensed by the sensor upon actions relating to of authorized access (Paragraph 0811) (through switch controlled by the Network Surveillance and Security System, “NSSS” **18**) to one or more digital assets by an end user of the end user client device;

an atomic level event aggregator (Paragraph 0435) configured to determine the occurrence of an aggregate event that comprises more than one atomic level asset

access event (Id.); and

a policy violation detector configured to determine whether an aggregate event has occurred that violates a predefined digital asset usage policy (Paragraph 0435) that indicates a risk of use of a digital asset outside the security perimeter (Paragraph 0224).

20. As to claims 2 and 13, Carter further shows:
the step of asserting the policy violation predicate is implemented in an operating system kernel of the client user device (Paragraphs 0810-0817) .

21. As to claim 3, Carter further shows:
preventing a user from accessing the digital asset if the policy predicate indicates a violated policy (Paragraph 1040).

22. As to claims 4 and 15, Carter further shows:
the preventing step includes an IRP intercept (Paragraph 0147, interrupt handler within the kernel).

23. As to claims 5 and 16, Carter further shows:
the combined event is a time sequence of multiple atomic level events (Paragraph 0224).

24. As to claims 7 and 18, Carter further shows:

asserting multiple policy violation predicates (Paragraph 0435) prior to indicating a risk of use of the digital asset outside of the security perimeter (Paragraph 0224).

25. As to claims 8 and 19, Carter further shows:
operates independently of application software (It is within the kernel, which is part of the Operating System, not the application software).

26. As to claims 10 and 21, Carter further shows:
the sensors, aggregators, and asserting steps operate in real time (Abstract, real time updating of the knowledge base requires that the sensors, aggregators, and asserting of predicates also operate in real time).

27. As to claims 11 and 22, Carter further shows:
determining the identity of a particular file in the asset access event (Paragraph 0162, In order to access the remote file through the local file, the system needs to determine the identity of the remote file.).

28. As to claim 14, Carter further shows
the policy violation detector determines a violated policy type (Shown as classes of violations in the table following paragraph 0787).

Claim Rejections - 35 USC § 103

29. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

30. Claim 9, as understood by the Examiner, is rejected under 35 U.S.C. §103(a) as being unpatentable over Carter in view of Danieli (US 6,510,513).

31. As to claim 9, Carter shows all of the elements of claim 1, but does not directly show the notification of the user that they have violated a policy. Danieli teaches "alerting a user of the client computer of the inappropriate use" (see claim 14). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the invention of Carter by adding the teachings of Danieli to make it known to the user that there was a violation, because the notification allows the user to know they have done something the system believes they should not, enabling them to justify their actions to a responsible party and possibly get the policy changed, if their actions were justified.

32. Claims 6, 17, and 20, as understood by the Examiner, are rejected under 35 U.S.C. §103(a) as being unpatentable over Carter in view of Admitted Prior Art.

33. As to claims 6, 17, and 20, Carter shows all of the elements except for the ability of the user to document their reason for the policy violation. It is considered admitted prior art that documenting the reason for an access is old and well known in the art. It therefore would have

been obvious to one of ordinary skill in the art at the time of the invention to modify the invention of Carter to incorporate this functionality. The ability to document the reason at the time of the occurrence would provide for a record of what was done and why, saving the effort of finding the appropriate person to notify.

34. Claims 1-5, 7, 8, 10-13, 15, 16, 18, 19, 21, and 22, as understood by the Examiner, are *alternatively* rejected under 35 USC 103(a) by Carter in view of Danieli.

35. As to claims 1 and 12, the Examiner primary position that it is inherent in Carter that the digital asset is used outside of the perimeter because the workstation using the asset is outside of the secure switch (Figure 1). However if not inherent, it is the Examiner's alternate position that Danieli clearly shows the process of securing a digital asset outside of the perimeter (Figure 6). Therefore, if not inherent, it would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the teachings of Carter to include the external security method of Danieli in order to extend the range of control over the digital assets past the security perimeter.

36. As to claims 2 and 13, Carter further shows:
the step of asserting the policy violation predicate is implemented in an operating system
kernel of the client user device (element 1018, figure 10) .

37. As to claim 3, Carter further shows:

preventing a user from accessing the digital asset if the policy predicate indicates a violated policy (Paragraph 1040).

38. As to claims 4 and 15, Carter further shows:
the preventing step includes an IRP intercept (Paragraph 0147, interrupt handler within the kernel).
39. As to claims 5 and 16, Carter further shows:
the combined event is a time sequence of multiple atomic level events (Paragraph 0224).
40. As to claims 7 and 18, Carter further shows:
asserting multiple policy violation predicates (Paragraph 0435) prior to indicating a risk of use of the digital asset outside of the security perimeter (Paragraph 0224).
41. As to claims 8 and 19, Carter further shows:
operates independently of application software (It is within the kernel, which is part of the Operating System, not the application software).
42. As to claims 10 and 21, Carter further shows:
the sensors, aggregators, and asserting steps operate in real time (Abstract, real time updating of the knowledge base requires that the sensors, aggregators, and asserting of predicates also operate in real time).

43. As to claims 11 and 22, Carter further shows:

determining the identity of a particular file in the asset access event (Paragraph 0162, In order to access the remote file through the local file, the system needs to determine the identity of the remote file.).

44. As to claim 14, Carter further shows

the policy violation detector determines a violated policy type (Shown as classes of violations in the table following paragraph 0787).

Terminal Disclaimer

45. The terminal disclaimer filed on 11 September 2008 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of 31 December 2023 has been reviewed and is accepted. The terminal disclaimer has been recorded.

Response to Arguments

46. Applicant's arguments filed 11 September 2008 have been fully considered but they are not persuasive.

47. Applicants argue:

“Applicants respectfully submit that functional language in an apparatus or system claim can be given patentable weight and that the language of the above system claims, as now recited,

is believed to clearly define and sufficiently describe the structure of the claimed invention. For example, system Claim 12 now recites that its structural components are "configured" in a particular way, much like the above example" (Remarks, Page 7).

48. Examiner's response:

In the excerpt provided by Applicants, it is noted that the limitations "serve to precisely define present **structural attributes of interrelated component parts**" (Remarks, Page 7) (emphasis added). However as used in the present claims, "configured to" is only used to show the functionality that can be performed by the component. There is no structure being imparted as all the structure needed to perform the functionality (processor, memory, communications means, etc.) is necessarily present in the device. Moreover, the configuring does not structurally change the interrelation of these parts.

Additionally, Applicants' use of "configured to..." removes the positive recitation of the action. A device can be configured to do something without actually having to do it.

The Examiner, in hopes of resolving this issue, suggests using the word "programmed" in place of "configured." In order for a device to perform any action, it has to be programmed, either in hardware or software. In this case Applicants have described operation from within the kernel of the operating system. Clearly, there is no ground for a new matter rejection on the use of "programmed to." Also, as the software is necessarily present in the instant claims, the scope lost by such an amendment should be negligible. However, the positive recitation of the software components in an apparatus or system claim is given patentable weight.

49. Applicants argue:

“In contrast to the system of Carter, users of the claimed process and system are already authorized users and already have access to digital assets within the network” (Remarks, Page 9, Paragraph 2).

50. Examiner's response:

The Examiner has cited paragraph 0811 in the rejection of this limitation, wherein Carter shows the allowing of authorized users to access the data. Moreover, it appears Applicants are asserting there is somehow a difference between the denying of access of one user and another. Regardless of the permissions of the user to perform other actions, if access is denied, the action has been deemed unauthorized. Paragraphs 0810-0817 detail multiple outcomes to sensed actions. These outcomes include: allowing actions if the user is authorized, restricting the action if the user is unauthorized, and more closely monitoring the actions if it is deemed necessary.

51. Applicants argue:

“As presented above, the Office asserts that the events of Carter are sensed at a switch controlled by Carter's NSSS (see Carter, reference numeral 18 of Fig. 1). The Office also asserts that a workstation of Carter's Fig. 1 discloses the claimed end user client device. If Carter's NSSS senses events at the switch of Fig. 1, then the NSSS does not sense events at a workstation of Fig. 1” (Remarks, Page 10, Paragraph 2).

52. Examiner's response:

There are alternate interpretations of the limitation this argument is made to. As noted above in the rejection under 35 U.S.C. 112 2nd paragraph, the interpretations argued is not the one taken by the Examiner. Because this interpretation is not required, arguments to the interpretation are not persuasive.

Conclusion

53. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 C.F.R. §1.136(a).

54. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 C.F.R. §1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

55. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JOSHUA MURDOUGH whose telephone number is (571)270-3270. The examiner can normally be reached on Monday - Thursday, 7:00 a.m. - 5:00 p.m.

56. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Fischer can be reached on (571) 272-6779. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

57. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Joshua Murdough
Examiner, Art Unit 3621

/ANDREW J. FISCHER/
Supervisory Patent Examiner, Art Unit 3621